

# A New Criterion on Normal Bases of Finite Field Extensions

Aixian Zhang<sup>a,\*</sup>, Keqin Feng<sup>b</sup>

<sup>a</sup>Department of Mathematical Sciences, Xi'an University of Technology, Shanxi, 710048, China.

<sup>b</sup>Department of Mathematical Sciences, Tsinghua University, Beijing, 100084, China.

---

## Abstract

A new criterion on normal bases of finite field extension  $\mathbb{F}_{q^n}/\mathbb{F}_q$  is presented and explicit criterions for several particular finite field extensions are derived from this new criterion.

**Keywords:** Normal basis, finite field, idempotent.

---

## 1. Introduction

The determination of normal bases for finite field extensions is one of the important topics in applications such as coding, cryptography and practical computation, particularly multiplication operation in finite fields.

A series of criterions on normal bases has been given ([11, 18]), many series of normal bases with lower complexity have been found ([1, 3, 5, 6, 9, 10, 12, 17, 20]), and explicit description to construct normal bases for specific cases of finite field have been presented ([2, 4, 8, 14, 15, 16, 19]).

In this paper we present a new criterion on normal bases for general case of extension  $\mathbb{F}_{q^n}/\mathbb{F}_q$  in Section 2. As applications of this new criterion, we show several examples in Section 3 which give explicit description of the normal bases for several specific extension of finite fields including previous results in ([14, 15, 19]).

## 2. A New Criterion on Normal Basis Generators for Finite Field Extensions

Let  $q = p^l$  be a power of prime number  $p, l \geq 1$ ,  $\mathbb{F}_q$  be the finite field with  $q$  elements. An element  $\alpha \in \mathbb{F}_{q^n}$  is called a normal basis generator (NBG) for extension  $\mathbb{F}_{q^n}/\mathbb{F}_q$  if  $\mathbf{B} = \{\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{n-1}}\}$  is a  $\mathbb{F}_q$ -basis of  $\mathbb{F}_{q^n}$ . In this case,  $\mathbf{B}$  is called a normal basis for  $\mathbb{F}_{q^n}/\mathbb{F}_q$ .

The normal bases for  $\mathbb{F}_{q^n}/\mathbb{F}_q$  are closely related to the ring of  $q$ -polynomial which we introduce now briefly. For more information on normal bases and  $q$ -polynomial we refer to books [11, 18].

A  $q$ -polynomial (or called linearized polynomial) is a polynomial in the following form:

$$L(x) = a_0x + a_1x^q + a_2x^{q^2} + \dots + a_mx^{q^m} \quad (a_i \in \mathbb{F}_q).$$

---

\*Corresponding author

Email addresses: zhangaixian1008@126.com (Aixian Zhang), kfeng@math.tsinghua.edu.cn (Keqin Feng)

Let  $\mathcal{F}_q[x]$  be the set of all  $q$ -polynomials. Then  $\mathcal{F}_q[x]$  is a ring with respect to the ordinary addition and the following multiplication  $\otimes$  :

$$L(x) \otimes K(x) = L(K(x)) \quad (\text{composition}).$$

One of basic facts on  $\mathcal{F}_q[x]$  is that the mapping

$$\phi : \mathbb{F}_q[x] \rightarrow \mathcal{F}_q[x], \quad \sum_{i=0}^m a_i x^i \mapsto \sum_{i=0}^m a_i x^{q^i} \quad (a_i \in \mathbb{F}_q)$$

is an isomorphism of rings. Therefore  $\mathcal{F}_q[x]$  is a principal ideal domain with identity  $x$ . We use the notation  $\parallel$  to express the divisibility in  $\mathcal{F}_q[x]$ . Namely, for  $L(x)$  and  $M(x)$  in  $\mathcal{F}_q[x]$ ,  $L(x) \parallel M(x)$  means that  $L(x) \neq 0$  and there exists  $N(x) \in \mathcal{F}_q[x]$  such that  $M(x) = L(x) \otimes N(x) = N(x) \otimes L(x)$ .

Let  $n$  be a positive integer. For  $\alpha \in \mathbb{F}_{q^n}$ , the set

$$I_\alpha = \{M(x) \in \mathcal{F}_q[x] : M(\alpha) = 0\}$$

is a nonzero ideal of  $\mathcal{F}_q[x]$  and  $x^{q^n} - x \in I_\alpha$ . The monic generator  $M_\alpha(x)$  of the ideal  $I_\alpha$  is called the minimal  $q$ -polynomial of  $\alpha$  over  $\mathbb{F}_q$ . Particularly,  $M_\alpha(x)$  is an irreducible polynomial in  $\mathcal{F}_q[x]$  and  $M_\alpha(x) \parallel x^{q^n} - x$ . Let  $x^n - 1$  has the following standard decomposition in  $\mathbb{F}_q[x]$  :

$$x^n - 1 = p_1(x)^{a_1} p_2(x)^{a_2} \cdots p_r(x)^{a_r}, \quad (1)$$

where  $p_1(x), p_2(x), \dots, p_r(x)$  are distinct monic irreducible polynomials in  $\mathbb{F}_q[x]$  and  $a_i \geq 1$  ( $1 \leq i \leq r$ ). Then the standard decomposition of  $x^{q^n} - x = \phi(x^n - 1)$  in  $\mathcal{F}_q[x]$  is

$$x^{q^n} - x = P_1(x)^{a_1} \otimes P_2(x)^{a_2} \otimes \cdots \otimes P_r(x)^{a_r},$$

where  $P_i(x) = \phi(p_i(x))$  ( $1 \leq i \leq r$ ) are distinct monic irreducible  $q$ -polynomials in  $\mathcal{F}_q[x]$ .

An element  $\alpha \in \mathbb{F}_{q^n}$  is a NBG of  $\mathbb{F}_{q^n}/\mathbb{F}_q$  means, by definition  $\{\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{n-1}}\}$  is  $\mathbb{F}_q$ -linear independent. This is also equivalent to that there is no non-zero  $q$ -polynomial  $G(x) = \sum_{i=0}^{n-1} c_i x^{q^i}$  ( $c_i \in \mathbb{F}_q$ ) such that  $G(x) \parallel x^{q^n} - x$  and  $G(\alpha) = 0$ . From this we give the following usual criterions on  $\alpha \in \mathbb{F}_{q^n}$  being a NBG of  $\mathbb{F}_{q^n}/\mathbb{F}_q$ .

**Theorem 2.1.** ([11, 18]) Suppose that  $x^n - 1$  has the decomposition (1) in  $\mathbb{F}_q[x]$ . Let  $l_i(x) = \frac{x^n - 1}{p_i(x)}$  and  $L_i(x) = \phi(l_i(x))$  ( $1 \leq i \leq r$ ). Then for  $\alpha \in \mathbb{F}_{q^n}$ ,  $\alpha$  is a NBG of  $\mathbb{F}_{q^n}/\mathbb{F}_q$  if and only if one of the following conditions satisfied

- (1) The minimal  $q$ -polynomial  $M_\alpha(x)$  of  $\alpha$  is  $x^{q^n} - x$ .
- (2) For each factor  $m(x)$  of  $x^n - 1$  in  $\mathbb{F}_q[x]$  with degree  $< n$  and  $M(x) = \phi(m(x))$ ,  $M(\alpha) \neq 0$ .
- (3)  $L_i(\alpha) \neq 0$  ( $1 \leq i \leq r$ ).

The criterions presented in Theorem 2.1 heavily depend on the decomposition (1) of  $x^n - 1$ . Now we present a new criterion on NBG of  $\mathbb{F}_{q^n}/\mathbb{F}_q$  which we use the  $q$ -equivalent classes of the elements in  $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ . To compute these  $q$ -equivalent classes is easier than to find the decomposition of  $x^n - 1$  in  $\mathbb{F}_q[x]$ .

Firstly we assume that  $(n, q) = 1$  (The other case can be easily reduced to  $(n, q) = 1$  case, see Theorem 3.10). Then the decomposition of  $x^n - 1$  in  $\mathbb{F}_q[x]$  is

$$x^n - 1 = p_1(x) p_2(x) \cdots p_r(x), \quad (2)$$

where  $p_i(x)$  ( $1 \leq i \leq r$ ) are distinct monic irreducible polynomials in  $\mathbb{F}_q[x]$ . The ring  $\mathbf{R} = \mathbb{F}_q[x]/(x^n - 1)$  is semi-simple and, by Chinese Remainder Theorem, is a direct sum of finite fields:

$$\mathbf{R} = \frac{\mathbb{F}_q[x]}{(x^n - 1)} \cong \oplus_{i=1}^r \frac{\mathbb{F}_q[x]}{(p_i(x))} \cong \oplus_{i=1}^r \mathbb{F}_{q^{d_i}}, \quad (3)$$

where  $d_i = \deg p_i(x)$  ( $1 \leq i \leq r$ ). Let  $\zeta$  be a fixed  $n$ -th primitive root of 1 in the algebraic closure of  $\mathbb{F}_q$ . Then  $Z_n$  is partitioned into  $r$   $q$ -classes

$$\begin{aligned} S_1 &= \{a_1 = 0\} \\ S_2 &= \{a_2, a_2q, \dots, a_2q^{d_2-1}\} \quad (a_2q^{d_2} = a_2 \in Z_n) \\ &\vdots \\ S_r &= \{a_r, a_rq, \dots, a_rq^{d_r-1}\} \quad (a_rq^{d_r} = a_r \in Z_n) \end{aligned} \quad (4)$$

and the roots  $\{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\}$  of  $x^n - 1$  are partitioned into  $r$   $\mathbb{F}_q$ -conjugate classes:

$$\begin{aligned} \mathcal{A}_1 &= \{\alpha_1 = 1\} \\ \mathcal{A}_2 &= \{\alpha_2, \alpha_2^q, \dots, \alpha_2^{q^{d_2-1}}\} \\ &\vdots \\ \mathcal{A}_r &= \{\alpha_r, \alpha_r^q, \dots, \alpha_r^{q^{d_r-1}}\}, \end{aligned}$$

where  $\alpha_i = \zeta^{a_i}$ ,  $d_i = \deg p_i(x)$  and  $\mathcal{A}_i$  is the set of roots of  $p_i(x)$  ( $1 \leq i \leq r, p_1(x) = x - 1$ ).

Our new criterion on NBG for  $\mathbb{F}_{q^n}/\mathbb{F}_q$  is expressed in terms of the orthogonal idempotent elements  $e_i(x) \in \mathbb{F}_q[x]$ ,  $\deg e_i(x) \leq n - 1$  ( $1 \leq i \leq r$ ) satisfying

$$e_i(x) \equiv \delta_{ij} \pmod{p_j(x)} \quad (1 \leq i, j \leq r), \quad (5)$$

where  $\delta_{ij}$  is the Kronecker symbol.

By Chinese Remainder Theorem, such idempotents  $e_i(x)$  ( $1 \leq i \leq r$ ) exist and uniquely determined. From (5) we get

$$e_i(\alpha_j) = \delta_{ij} \quad (1 \leq i, j \leq r) \quad (6)$$

and have the following orthogonal idempotent decomposition in  $\mathbf{R} = \frac{\mathbb{F}_q[x]}{(x^n - 1)}$ ,

$$1 = e_1(x) + \dots + e_r(x), \quad e_i(x)e_j(x) = \delta_{ij}e_i(x) \quad (1 \leq i, j \leq r). \quad (7)$$

Let  $E_i(x) = \phi(e_i(x)) \in \frac{\mathcal{F}_q[x]}{(x^{q^n} - x)}$  ( $1 \leq i \leq r$ ). Our new criterion on NBG for  $\mathbb{F}_{q^n}/\mathbb{F}_q$  is the following fundamental result.

**Theorem 2.2.** *Let  $e_i(x)$  ( $1 \leq i \leq r$ ) be the idempotent elements in  $\mathbf{R} = \frac{\mathbb{F}_q[x]}{(x^n - 1)}$  defined by (5).  $E_i(x) = \phi(e_i(x)) \in \frac{\mathcal{F}_q[x]}{(x^{q^n} - x)}$ . Then for  $\alpha \in \mathbb{F}_{q^n}$ ,  $\alpha$  is a NBG for  $\mathbb{F}_{q^n}/\mathbb{F}_q$  if and only if  $E_i(\alpha) \neq 0$  ( $1 \leq i \leq r$ ).*

*Proof.* Let  $l_i(x) = \frac{x^n - 1}{p_i(x)}$ ,  $L_i(x) = \phi(l_i(x))$  ( $1 \leq i \leq r$ ). From Theorem 2.1 we know that  $\alpha$  is a NBG for  $\mathbb{F}_{q^n}/\mathbb{F}_q$  if and only if  $L_i(\alpha) \neq 0$  ( $1 \leq i \leq r$ ). Now we claim that for each  $i$  ( $1 \leq i \leq r$ ),

$$L_i(\alpha) = 0 \Leftrightarrow E_i(\alpha) = 0.$$

From this the Theorem 2.2 follows.

From (5) we get

$$l_i(x) \equiv l_i(x)e_i(x) \pmod{x^n - 1}.$$

By the isomorphism  $\varphi : \mathbb{F}_q[x] \rightarrow \mathcal{F}_q[x]$  we get the following congruences in ring  $\mathcal{F}_q[x]$  :

$$L_i(x) \equiv L_i(x) \otimes E_i(x) \pmod{x^{q^n} - x}.$$

Then by  $\alpha^{q^n} = \alpha$  we get

$$L_i(\alpha) = L_i(x) \otimes E_i(x) \big|_{x=\alpha} = L_i(E_i(\alpha)).$$

Particularly, if  $E_i(\alpha) = 0$ , then  $L_i(\alpha) = L_i(0) = 0$ .

Conversely, the fact  $(l_i(x), p_i(x)) = 1$  in  $\mathbb{F}_q[x]$  implies that there exist  $a(x), b(x) \in \mathbb{F}_q[x]$  such that  $a(x)l_i(x) + b(x)p_i(x) = 1$ . Therefore

$$\begin{aligned} e_i(x) &= e_i(x)a(x)l_i(x) + e_i(x)b(x)p_i(x) \\ &\equiv e_i(x)a(x)l_i(x) \pmod{x^n - 1}, \end{aligned}$$

since  $e_i(x)p_i(x) \equiv 0 \pmod{x^n - 1}$  by (5). Therefore in  $\mathcal{F}_q[x]$ ,  $E_i(x) \equiv E_i(x) \otimes A(x) \otimes L_i(x) \pmod{x^{q^n} - x}$ , where  $A(x) = \varphi(a(x))$ . Therefore  $L_i(\alpha) = 0$  implies that  $E_i(\alpha) = 0$ . This completes the proof of Theorem 2.2.  $\square$

Next we present a rather easy method to compute the idempotents  $e_i(x)$  and so  $E_i(x) = \varphi(e_i(x))$  ( $1 \leq i \leq r$ ).

**Theorem 2.3.** *Let*

$$\varepsilon_i(x) = \sum_{a \in \mathcal{S}_i} x^a$$

where  $\mathcal{S}_i$  ( $1 \leq i \leq r$ ) are  $q$ -classes of  $\mathbb{Z}_n$  are defined by partition (4),  $\alpha_i \in \mathcal{A}_i$  and  $\mathbf{M}$  is an  $r \times r$  matrix over  $\mathbb{F}_q$  defined by

$$\mathbf{M} = (\varepsilon_i(\alpha_j))_{1 \leq i, j \leq r}.$$

Then  $\det(\mathbf{M}) \neq 0$  and

$$\begin{pmatrix} e_1(x) \\ \vdots \\ e_r(x) \end{pmatrix} = \mathbf{M}^{-1} \begin{pmatrix} \varepsilon_1(x) \\ \vdots \\ \varepsilon_r(x) \end{pmatrix}. \quad (8)$$

*Proof.* Firstly we prove that  $\varepsilon_i(\alpha_j) \in \mathbb{F}_q$  ( $1 \leq i, j \leq r$ ). Since  $\alpha_j = \zeta^{a_j}$ , we have  $\varepsilon_i(\alpha_j) = \sum_{\lambda=0}^{d_i-1} \zeta^{a_j a_i q^\lambda}$  and

$$\begin{aligned} \varepsilon_i(\alpha_j)^q &= \sum_{\lambda=0}^{d_i-1} (\zeta^{a_j a_i q^{\lambda+1}})^{a_j} \\ &= \sum_{\lambda=0}^{d_i-1} (\zeta^{a_j a_i q^\lambda})^{a_j} = \varepsilon_i(\alpha_j). \end{aligned}$$

Therefore  $\varepsilon_i(\alpha_j) \in \mathbb{F}_q$  and  $\mathbf{M}$  is a matrix over  $\mathbb{F}_q$ . By the definition of  $\varepsilon_i(x)$  we know that

$$\varepsilon_i(x) \equiv x^{a_i} + x^{a_i q} + \cdots + x^{a_i q^{d_i-1}} \pmod{x^n - 1} \quad (1 \leq i \leq r).$$

Then by (7) we have  $e_i(x)^q \equiv e_i(x) \pmod{x^n - 1}$ . Therefore  $e_i(x)$  is a  $\mathbb{F}_q$ -linear combination of  $\varepsilon_1(x), \varepsilon_2(x), \dots, \varepsilon_r(x)$ . Namely,

$$\begin{pmatrix} e_1(x) \\ \vdots \\ e_r(x) \end{pmatrix} = \mathbf{A} \begin{pmatrix} \varepsilon_1(x) \\ \vdots \\ \varepsilon_r(x) \end{pmatrix},$$

where  $\mathbf{A}$  is an  $r \times r$  matrix over  $\mathbb{F}_q$ . By using (6), we get

$$\mathbf{I}_r = \begin{pmatrix} e_1(\alpha_1) & \cdots & e_1(\alpha_r) \\ \vdots & & \vdots \\ e_r(\alpha_1) & \cdots & e_r(\alpha_r) \end{pmatrix} = \mathbf{A} \begin{pmatrix} \varepsilon_1(\alpha_1) & \cdots & \varepsilon_1(\alpha_r) \\ \vdots & & \vdots \\ \varepsilon_r(\alpha_1) & \cdots & \varepsilon_r(\alpha_r) \end{pmatrix} = \mathbf{A}\mathbf{M}.$$

Therefore  $\det(\mathbf{M}) \neq 0$  and  $\mathbf{A} = \mathbf{M}^{-1}$ . This completes the proof of the Theorem 2.3.  $\square$

### 3. Examples

**Example 3.1.** Let  $n$  be a prime number,  $q = p^m$ ,  $n \neq p$ . Suppose that  $q$  is a primitive root of  $n$  which means that  $(\mathbb{Z}/n\mathbb{Z})^* = \langle q \rangle$ . Let  $\zeta$  be an  $n$ -th primitive root of 1 so that  $\mathbb{F}_q(\zeta) = \mathbb{F}_{q^{n-1}}$ . Then  $x^n - 1$  is decomposed in  $\mathbb{F}_q[x]$  as

$$x^n - 1 = (x - 1)p_2(x),$$

where  $p_2(x) = x^{n-1} + x^{n-2} + \cdots + x + 1$  is irreducible in  $\mathbb{F}_q[x]$ . The  $\mathbb{F}_q$ -conjugate classes of  $\{\zeta^\lambda : 0 \leq \lambda \leq n-1\}$  are

$$\begin{aligned} \mathcal{A}_1 &= \{1\}, \alpha_1 = 1 \\ \mathcal{A}_2 &= \{\zeta^{q^l} : 0 \leq l \leq n-2\} = \{\zeta^\lambda : 1 \leq \lambda \leq n-1\}. \end{aligned}$$

Therefore  $\varepsilon_1(x) = 1$ ,  $\varepsilon_2(x) = x + x^2 + \cdots + x^{n-1}$ , and

$$\mathbf{M} = \begin{pmatrix} \varepsilon_1(1) & \varepsilon_1(\zeta) \\ \varepsilon_2(1) & \varepsilon_2(\zeta) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ n-1 & -1 \end{pmatrix}, \mathbf{M}^{-1} = \frac{1}{n} \begin{pmatrix} 1 & 1 \\ n-1 & -1 \end{pmatrix}.$$

Therefore by (8),

$$\begin{aligned} e_1(x) &= \frac{1}{n}(\varepsilon_1(x) + \varepsilon_2(x)) = \frac{1}{n}(1 + x + x^2 + \cdots + x^{n-1}) \\ e_2(x) &= \frac{1}{n}((n-1)\varepsilon_1(x) - \varepsilon_2(x)) = 1 - \frac{1}{n}(1 + x + x^2 + \cdots + x^{n-1}) = 1 - e_1(x), \end{aligned}$$

and

$$E_1(x) = \frac{1}{n} \left( \sum_{i=0}^{n-1} x^{q^i} \right), \quad E_2(x) = x - E_1(x).$$

Let  $\text{Tr}$  be the trace mapping for  $\mathbb{F}_{q^n}/\mathbb{F}_q$ . Namely, for  $\alpha \in \mathbb{F}_{q^n}$ ,

$$\text{Tr}(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i} = nE_1(\alpha).$$

Therefore,

$$E_1(\alpha) = \frac{1}{n}\text{Tr}(\alpha), \quad E_2(\alpha) = \alpha - \frac{1}{n}\text{Tr}(\alpha).$$

By Theorem 2.2, for  $\alpha \in \mathbb{F}_{q^n}$ ,

$$\begin{aligned} \alpha \text{ is a NBG for } \mathbb{F}_{q^n}/\mathbb{F}_q &\Leftrightarrow E_1(\alpha) \neq 0 \text{ and } E_2(\alpha) \neq 0 \\ &\Leftrightarrow \text{Tr}(\alpha) \neq 0 \text{ and } n\alpha \neq \text{Tr}(\alpha) \in \mathbb{F}_q \\ &\Leftrightarrow \text{Tr}(\alpha) \neq 0 \text{ and } \alpha \notin \mathbb{F}_q \text{ (since } \alpha \in \mathbb{F}_q \text{ implies that } n\alpha = \text{Tr}(\alpha)). \end{aligned}$$

Therefore we get the following result given by Pei et al. in [15].

**Theorem 3.2.** Let  $q = p^m$ ,  $n$  be a prime number,  $n \neq p$ . If  $(\mathbb{Z}/n\mathbb{Z})^* = \langle q \rangle$ . Then for  $\alpha \in \mathbb{F}_{q^n}$ ,  $\alpha$  is a NBG for  $\mathbb{F}_{q^n}/\mathbb{F}_q$  if and only if  $\alpha \notin \mathbb{F}_q$  and  $\text{Tr}(\alpha) \neq 0$ , where  $\text{Tr}$  is the trace mapping for  $\mathbb{F}_{q^n}/\mathbb{F}_q$ .

**Example 3.3.** Let  $n$  be an odd prime number,  $n \neq p$ ,  $q = p^m$ . Suppose that the (multiplicative) order of  $q$  in  $(\mathbb{Z}/n\mathbb{Z})^*$  is  $l = \frac{\Phi(n)}{2} = \frac{n-1}{2}$  so that in  $(\mathbb{Z}/n\mathbb{Z})^*$ ,

$$\{q^\lambda : 0 \leq \lambda \leq l-1\} = \{1 \leq r \leq n-1 : \left(\frac{r}{n}\right) = 1\},$$

where  $\left(\frac{r}{n}\right)$  is the Legendre symbol.

Let  $\zeta$  be an  $n$ -th primitive root of 1 in the algebraic closure of  $\mathbb{F}_q$  so that  $\mathbb{F}_q(\zeta) = \mathbb{F}_{q^l}$ . The conjugate classes of  $\{1, \zeta, \dots, \zeta^{n-1}\}$  are

$$\begin{aligned} \mathcal{A}_1 &= \{1\}, \alpha_1 = 1, \\ \mathcal{A}_2 &= \{\zeta^r : 1 \leq r \leq n-1, \left(\frac{r}{n}\right) = 1\}, \alpha_2 = \zeta, \\ \mathcal{A}_3 &= \{\zeta^r : 1 \leq r \leq n-1, \left(\frac{r}{n}\right) = -1\}, \alpha_3 = \zeta^g, \end{aligned}$$

where  $g$  is a generator of the cyclic group  $(\mathbb{Z}/n\mathbb{Z})^*$ . Therefore

$$\varepsilon_1(x) = 1, \varepsilon_2(x) = \sum_{\substack{r=1 \\ \left(\frac{r}{n}\right)=1}}^{n-1} x^r, \varepsilon_3(x) = \sum_{\substack{r=1 \\ \left(\frac{r}{n}\right)=-1}}^{n-1} x^r. \quad (9)$$

$$\mathbf{M} = \begin{pmatrix} \varepsilon_1(1) & \varepsilon_1(\zeta) & \varepsilon_1(\zeta^g) \\ \varepsilon_2(1) & \varepsilon_2(\zeta) & \varepsilon_2(\zeta^g) \\ \varepsilon_3(1) & \varepsilon_3(\zeta) & \varepsilon_3(\zeta^g) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ l & C & B \\ l & B & C \end{pmatrix},$$

where

$$C = \sum_{\substack{r=1 \\ \left(\frac{r}{n}\right)=1}}^{n-1} \zeta^r \in \mathbb{F}_q, B = \sum_{\substack{r=1 \\ \left(\frac{r}{n}\right)=-1}}^{n-1} \zeta^r = -1 - C,$$

and

$$\mathbf{M}^{-1} = \frac{1}{n(B-C)} \begin{pmatrix} B-C & B-C & B-C \\ l(B-C) & C-l & l-B \\ l(B-C) & l-B & C-l \end{pmatrix}.$$

From (8) we get

$$\begin{cases} ne_1(x) = \varepsilon_1(x) + \varepsilon_2(x) + \varepsilon_3(x) = \sum_{i=0}^{n-1} x^i \\ n(B-C)e_2(x) = l(B-C) + (C-l)\varepsilon_2(x) + (l-B)\varepsilon_3(x) \\ n(B-C)e_3(x) = l(B-C) + (l-B)\varepsilon_2(x) + (C-l)\varepsilon_3(x). \end{cases} \quad (10)$$

Case (I):  $2 \nmid q$

Let  $n^* = (\frac{-1}{n})n$ . Then  $B-C = -\sum_{r=1}^{n-1} (\frac{r}{n})\zeta^r$  is the quadratic Gauss sum, but valued in  $\mathbb{F}_{q^l}$ . We have

$$\begin{aligned} (B-C)^2 &= \sum_{1 \leq r, s \leq n-1} (\frac{rs}{n})\zeta^{r+s} = \sum_{1 \leq t, s \leq n-1} (\frac{t}{n})\zeta^{s(t+1)} \\ &= -\sum_{t \neq -1} (\frac{t}{n}) + (n-1)(\frac{-1}{n}) = n^*. \end{aligned}$$

Therefore  $B-C = \mu\sqrt{n^*}$ ,  $\mu \in \{1, -1\}$ . Then from  $B+C = -1$ , we get

$$B = \frac{1}{2}(-1 + \mu\sqrt{n^*}), C = \frac{1}{2}(-1 - \mu\sqrt{n^*}).$$

By (10) and (9) we have

$$\begin{aligned} ne_1(x) &= \sum_{i=0}^{n-1} x^i, \\ n\mu\sqrt{n^*}e_2(x) &= l\mu\sqrt{n^*} + [(-\frac{1}{2} - \frac{\mu\sqrt{n^*}}{2}) - l]\varepsilon_2(x) + [l + (\frac{1}{2} - \frac{\mu\sqrt{n^*}}{2})]\varepsilon_3(x), \\ &= l\mu\sqrt{n^*} + \frac{n}{2}(\varepsilon_3(x) - \varepsilon_2(x)) - \frac{\mu\sqrt{n^*}}{2}(\varepsilon_3(x) + \varepsilon_2(x)) \\ n\mu\sqrt{n^*}e_3(x) &= l\mu\sqrt{n^*} - \frac{n}{2}(\varepsilon_3(x) - \varepsilon_2(x)) - \frac{\mu\sqrt{n^*}}{2}(\varepsilon_3(x) + \varepsilon_2(x)). \end{aligned}$$

Then  $E_i(x) = \Phi(e_i(x))$  ( $1 \leq i \leq 3$ ) are

$$\begin{aligned} nE_1(x) &= \sum_{i=0}^{n-1} x^{q^i}, \\ 2n\sqrt{n^*}E_2(x) &= 2l\sqrt{n^*}x - \mu n \sum_{r=1}^{n-1} (\frac{r}{n})x^{q^r} - \sqrt{n^*} \sum_{r=1}^{n-1} x^{q^r}, \\ 2n\sqrt{n^*}E_3(x) &= 2l\sqrt{n^*}x + \mu n \sum_{r=1}^{n-1} (\frac{r}{n})x^{q^r} - \sqrt{n^*} \sum_{r=1}^{n-1} x^{q^r}. \end{aligned}$$

Let  $\text{Tr}$  be the trace mapping for  $\mathbb{F}_{q^n}/\mathbb{F}_q$ . By Theorem 2.2 we get, for  $\alpha \in \mathbb{F}_{q^n}$ ,

$$\begin{aligned} \alpha \text{ is a NBG for } \mathbb{F}_{q^n}/\mathbb{F}_q &\Leftrightarrow E_i(\alpha) \neq 0 \ (1 \leq i \leq 3) \\ &\Leftrightarrow \text{Tr}(\alpha) \neq 0 \text{ and } 2l\sqrt{n^*}\alpha - \sqrt{n^*}(\text{Tr}(\alpha) - \alpha) \neq \pm n \sum_{r=1}^{n-1} \left(\frac{r}{n}\right) \alpha^{q^r} \\ &\Leftrightarrow \text{Tr}(\alpha) \neq 0 \text{ and } n\sqrt{n^*}\alpha - \sqrt{n^*}\text{Tr}(\alpha) \neq \pm n \sum_{r=1}^{n-1} \left(\frac{r}{n}\right) \alpha^{q^r}. \end{aligned}$$

Case (II):  $2 \mid q$ .

In this case  $B + C = B - C = 1$  and by (10)

$$\begin{aligned} ne_1(x) &= \sum_{i=0}^{n-1} x^i, \\ ne_2(x) &= l + (l + B)(\epsilon_2(x) + \epsilon_3(x)) + \epsilon_2(x), \\ ne_3(x) &= l + (l + B + 1)(\epsilon_2(x) + \epsilon_3(x)) + \epsilon_2(x). \end{aligned}$$

Therefore, for  $\alpha \in \mathbb{F}_{q^n}$ ,

$$\begin{aligned} nE_1(\alpha) &= \text{Tr}(\alpha), \\ nE_2(\alpha) &= l\text{Tr}(\alpha) + B(\text{Tr}(\alpha) + \alpha) + A, \\ nE_3(\alpha) &= l\text{Tr}(\alpha) + (B + 1)(\text{Tr}(\alpha) + \alpha) + A, \end{aligned}$$

where  $A = \sum_{\substack{r=1 \\ (\frac{r}{n})=1}}^{n-1} \alpha^{q^r}$ . Therefore for  $\alpha \in \mathbb{F}_{q^n}$ ,

$$\begin{aligned} \alpha \text{ is a NBG for } \mathbb{F}_{q^n}/\mathbb{F}_q &\Leftrightarrow \text{Tr}(\alpha) \neq 0, A \neq l\text{Tr}(\alpha) + B(\text{Tr}(\alpha) + \alpha) \\ &\text{and } A \neq l\text{Tr}(\alpha) + (B + 1)(\text{Tr}(\alpha) + \alpha). \end{aligned}$$

If  $n \equiv \pm 1 \pmod{8}$ , then  $(\frac{2}{n}) = 1$  and  $B^2 = \sum_{\substack{r=1 \\ (\frac{r}{n})=1}}^{n-1} \zeta^{2r} = B$ . Therefore  $B \in \{0, 1\}$ . If  $n \equiv \pm 3 \pmod{8}$ ,

then  $(\frac{2}{n}) = -1$  and  $B^2 = C = B + 1$ . Therefore  $B \in \{\omega, \omega + 1\}$  where  $\omega$  and  $\omega + 1$  are two roots of  $x^2 + x + 1$  in  $\mathbb{F}_4$ . Thus we get the following result.

**Theorem 3.4.** Let  $n$  be an odd prime number,  $n \neq p$ ,  $q = p^m$ ,  $\text{Tr}$  be the trace mapping for  $\mathbb{F}_{q^n}/\mathbb{F}_q$ ,  $n^* = (\frac{-1}{n})n$ . Suppose that the (multiplicative) order of  $q$  in  $(\mathbb{Z}/n\mathbb{Z})^*$  is  $l = \frac{\phi(n)}{2} = \frac{n-1}{2}$ . Then for  $\alpha \in \mathbb{F}_{q^n}$ , we have the following criterion

(1) If  $p \geq 3$ ,  $\alpha$  is a NBG for  $\mathbb{F}_{q^n}/\mathbb{F}_q$  if and only if  $\text{Tr}(\alpha) \neq 0$  and  $\sqrt{n^*}(n\alpha - \text{Tr}(\alpha)) \neq \pm n \sum_{r=1}^{n-1} \left(\frac{r}{n}\right) \alpha^{q^r}$ .

(2) If  $p = 2$ ,  $\alpha$  is a NBG for  $\mathbb{F}_{q^n}/\mathbb{F}_q$  if and only if  $\text{Tr}(\alpha) \neq 0$  and

$$\begin{cases} A \neq l\text{Tr}(\alpha), (l + 1)\text{Tr}(\alpha) + \alpha, \text{ for } n \equiv \pm 1 \pmod{8} \\ A \neq l\text{Tr}(\alpha) + \omega(\text{Tr}(\alpha) + \alpha), l\text{Tr}(\alpha) + (\omega + 1)(\text{Tr}(\alpha) + \alpha), \text{ for } n \equiv \pm 3 \pmod{8}, \end{cases}$$



where  $A = \sum_{\substack{r=1 \\ (\frac{r}{n})=1}}^{n-1} \alpha^{q^r}$  and  $\{\omega, \omega + 1\}$  are two roots of  $x^2 + x + 1$  in  $\mathbb{F}_4$ .

Particularly, if  $q = p = 2$ , then  $\alpha \in \mathbb{F}_{2^n}$  is a NBG for  $\mathbb{F}_{2^n}/\mathbb{F}_2$  if and only if  $\text{Tr}(\alpha) = 1$  and  $\sum_{\substack{r=1 \\ (\frac{r}{n})=1}}^{n-1} \alpha^{q^r} \neq l, l + 1 + \alpha$ , where  $\text{Tr}$  is the trace mapping for  $\mathbb{F}_{2^n}/\mathbb{F}_2$ .

**Example 3.5.** (Generalization of Example 2) Let  $n$  and  $p$  be distinct prime numbers,  $q = p^m$ . Let  $f$  be the order of  $q$  in  $(\mathbb{Z}/n\mathbb{Z})^*$ ,  $n - 1 = ef$ . Then we have a generator of the cyclic group  $(\mathbb{Z}/n\mathbb{Z})^*$  such that  $q \equiv g^e \pmod{n}$  and  $(\mathbb{Z}/n\mathbb{Z})^*$  is partitioned into cyclotomic classes

$$C_i = \{g^{i+ej} : 0 \leq j \leq f-1\} \quad (0 \leq i \leq e-1).$$

Let  $\zeta$  be an  $n$ -th primitive root of 1,  $\mathbb{F}_q(\zeta) = \mathbb{F}_{q^f}$ . Then  $\{\zeta^a : 0 \leq a \leq n-1\}$  be partitioned into  $e+1$   $\mathbb{F}_q$ -conjugate classes

$$\begin{aligned} \mathcal{A}_* &= \{1\}, \alpha_* = 1 \\ \mathcal{A}_i &= \{\zeta^a : a \in C_i\}, \alpha_i = \zeta^{g^i} \quad (0 \leq i \leq e-1). \end{aligned}$$

Therefore

$$\epsilon_*(x) = 1, \quad \epsilon_i(x) \equiv \sum_{a \in C_i} x^a \pmod{x^n - 1}.$$

Let  $\epsilon_i = \epsilon_i(\zeta)$  ( $0 \leq i \leq e-1$ ). We know that  $\epsilon_i \in \mathbb{F}_q$  and

$$\epsilon_i(\alpha_j) = \sum_{a \in C_i} \zeta^{ag^j} = \epsilon_{i+j}.$$

Therefore

$$\mathbf{M} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ f & \epsilon_0 & \epsilon_1 & \cdots & \epsilon_{e-1} \\ f & \epsilon_1 & \epsilon_2 & \cdots & \epsilon_0 \\ \vdots & \vdots & \vdots & & \vdots \\ f & \epsilon_{e-1} & \epsilon_0 & \cdots & \epsilon_{e-2} \end{pmatrix}.$$

By using the equality

$$\begin{aligned} \sum_{i=0}^{e-1} \epsilon_i \epsilon_{i+j} &= \sum_{i=0}^{e-1} \sum_{a, b \in C_0} \zeta^{g^i(a+g^j b)} \\ &= \begin{cases} n-f, & \text{if } -1 \in C_j \ (\Leftrightarrow j \equiv \frac{ef}{2} \pmod{e}) \\ -f, & \text{otherwise.} \end{cases} \end{aligned}$$

We can get

$$\mathbf{M}^{-1} = \frac{1}{n} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ f & \epsilon_c & \epsilon_{c+1} & \cdots & \epsilon_{c-1} \\ f & \epsilon_{c+1} & \epsilon_{c+2} & \cdots & \epsilon_c \\ \vdots & \vdots & \vdots & & \vdots \\ f & \epsilon_{c-1} & \epsilon_c & \cdots & \epsilon_{c-2} \end{pmatrix},$$

where  $c \equiv \frac{ef}{2} \pmod{e}$ , namely

$$c = \begin{cases} \frac{e}{2}, & \text{if } 2 \mid e \text{ and } 2 \nmid f, \\ 0, & \text{otherwise.} \end{cases}$$

Therefore for  $\alpha \in \mathbb{F}_{q^n}$ ,

$$\begin{aligned} nE_*(\alpha) &= \text{Tr}(\alpha), \\ nE_j(\alpha) &= f\alpha + \sum_{i=0}^{e-1} \epsilon_{i+j} \sum_{a \in C_i} \alpha^{q^a} \quad (0 \leq j \leq e-1). \end{aligned}$$

Thus we get the following result.

**Theorem 3.6.** *Let  $n$  and  $p$  be distinct prime numbers,  $q = p^m$ . Let  $f$  be the order of  $q$  in  $(\mathbb{Z}/n\mathbb{Z})^*$ ,  $n-1 = ef$ . Let  $\zeta$  be an  $n$ -th primitive root of 1,  $\mathbb{F}_q(\zeta) = \mathbb{F}_{q^f}$ . We choose  $g \in \mathbb{Z}$  such that  $(\mathbb{Z}/n\mathbb{Z})^* = \langle g \rangle$  and  $q \equiv g^e \pmod{n}$ . We denote*

$$C_i = \{g^{i+ej} : 0 \leq j \leq f-1\} \quad (0 \leq i \leq e-1), \epsilon_i = \sum_{a \in C_i} \zeta^a \in \mathbb{F}_q \quad (0 \leq i \leq e-1).$$

Then for  $\alpha \in \mathbb{F}_{q^n}$ ,  $\alpha$  is a NBG for  $\mathbb{F}_{q^n}/\mathbb{F}_q$  if and only if  $\text{Tr}(\alpha) \neq 0$  and

$$\sum_{i=0}^{e-1} \epsilon_{i+j} \sum_{a \in C_i} \alpha^{q^a} \neq -f\alpha \quad (0 \leq j \leq e-1).$$

**Remark 3.7.** (1) The Gauss periods  $\epsilon_i$  ( $0 \leq i \leq e-1$ ) can be calculated explicitly for many cases of  $e$  ( $= 2, 3, 4, \dots$ ) by using Gauss sums so that more closer form of Theorem 3.6 can be derived for such  $e$ . Particularly, for  $e = 1$  and 2, we obtain Theorems 3.2 and 3.4.

(2) For  $q = 2, e = 3, 5, 7$  and  $q = 4, e = 3$ , we have  $\epsilon_i \in \mathbb{F}_2$  and

$$\sum_{i=0}^{e-1} \epsilon_i \epsilon_{i+j} = \begin{cases} 1, & \text{if } j = 0, \\ 0 & \text{if } 1 \leq j \leq e-1, \end{cases}$$

which means that the matrix

$$\begin{pmatrix} \epsilon_0 & \epsilon_1 & \cdots & \epsilon_{e-1} \\ \epsilon_1 & \epsilon_2 & \cdots & \epsilon_0 \\ \vdots & \vdots & & \vdots \\ \epsilon_{e-1} & \epsilon_0 & \cdots & \epsilon_{e-2} \end{pmatrix}$$

is an orthogonal circulate matrix over  $\mathbb{F}_2$ . Jungnickel et al. [7] obtained a formula on the number of orthogonal circulate  $e \times e$  matrices over  $\mathbb{F}_q$ . From this formula we know that there essentially exist unique such matrix for  $q = 2, e = 3, 5, 7$  and  $q = 4, e = 3$ . Namely,  $(\epsilon_0, \epsilon_1, \dots, \epsilon_{e-1}) = (1, 0, \dots, 0)$ .

In these cases, the conclusion of Theorem 3.6 can be simplified as :

$\alpha$  is a NBG for  $\mathbb{F}_{q^n}/\mathbb{F}_q$  if and only if  $\text{Tr}(\alpha) \neq 0$  and

$$\sum_{i=0}^{e-1} \epsilon_{i+j} \sum_{a \in C_i} \alpha^{q^a} \neq -f\alpha \quad (0 \leq j \leq e-1).$$

**Example 3.8.** Let  $p_1, p_2, p$  be distinct prime numbers,  $p_1 \geq 3, p_2 \geq 3, n = p_1 p_2, q = p^m$ . Suppose that  $(\mathbb{Z}/p_1\mathbb{Z})^* = \langle q \rangle, (\mathbb{Z}/p_2\mathbb{Z})^* = \langle q \rangle$  and  $(p_1 - 1, p_2 - 1) = 2$ . Then the order of  $q$  in  $(\mathbb{Z}/n\mathbb{Z})^*$  is  $f = \frac{(p_1-1)(p_2-1)}{2}$ . Let  $\zeta$  be a  $n$ -th root of 1 and  $\mathbb{F}_q(\zeta) = \mathbb{F}_{q^f}$ . The set  $\{\zeta^i : 0 \leq i \leq n-1\}$  be partitioned into five  $\mathbb{F}_q$ -conjugate classes as following:

$$\begin{aligned}\mathcal{A}_0 &= \{1\}, |\mathcal{A}_0| = 1, \alpha_0 = 1, \\ \mathcal{A}_1 &= \{\zeta, \zeta^q, \dots, \zeta^{q^{f-1}}\}, |\mathcal{A}_1| = f, \alpha_1 = \zeta, \\ \mathcal{A}_2 &= \{\zeta^g, \zeta^{qg}, \dots, \zeta^{q^{f-1}g}\}, |\mathcal{A}_2| = f, \alpha_2 = \zeta^g (\text{where } \zeta^g \notin \mathcal{A}_1 \text{ and } (g, n) = 1), \\ \mathcal{A}_3 &= \{\zeta^{p_1}, \zeta^{qp_1}, \dots, \zeta^{q^{p_2-2}p_1}\}, |\mathcal{A}_3| = p_2 - 1, \alpha_3 = \zeta^{p_1}, \\ \mathcal{A}_4 &= \{\zeta^{p_2}, \zeta^{qp_2}, \dots, \zeta^{q^{p_1-2}p_2}\}, |\mathcal{A}_4| = p_1 - 1, \alpha_4 = \zeta^{p_2}.\end{aligned}$$

Therefore

$$\begin{aligned}\varepsilon_0(x) &= 1, \varepsilon_1(x) = \sum_{i=0}^{f-1} x^{q^i}, \varepsilon_2(x) = \sum_{i=0}^{f-1} x^{gq^i}, \\ \varepsilon_3(x) &= \sum_{j=0}^{p_2-2} x^{q^j p_1}, \varepsilon_4(x) = \sum_{j=0}^{p_1-2} x^{q^j p_2}.\end{aligned}$$

$$\mathcal{M} = (\varepsilon_i(\alpha_j))_{0 \leq i, j \leq 4} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ f & \varepsilon_1 & \varepsilon_2 & -\frac{p_1-1}{2} & -\frac{p_2-1}{2} \\ f & \varepsilon_2 & \varepsilon_1 & -\frac{p_1-1}{2} & -\frac{p_2-1}{2} \\ p_2-1 & -1 & -1 & -1 & p_2-1 \\ p_1-1 & -1 & -1 & p_1-1 & -1 \end{pmatrix},$$

where  $\varepsilon_i = \varepsilon_i(\alpha_j) \in \mathbb{F}_q$  ( $i = 1, 2$ ).

If  $2 \nmid q$ , then

$$n\mathcal{M}^{-1} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 2m_1m_2 & \frac{n}{2(\varepsilon_1-\varepsilon_2)} + \frac{1}{2} & -\frac{n}{2(\varepsilon_1-\varepsilon_2)} + \frac{1}{2} & -m_1 & -m_2 \\ 2m_1m_2 & -\frac{n}{2(\varepsilon_1-\varepsilon_2)} + \frac{1}{2} & \frac{n}{2(\varepsilon_1-\varepsilon_2)} + \frac{1}{2} & -m_1 & -m_2 \\ 2m_2 & -1 & -1 & -1 & 2m_2 \\ 2m_1 & -1 & -1 & 2m_1 & -1 \end{pmatrix},$$

where  $m_i = \frac{p_i-1}{2}$  ( $i = 1, 2$ ). Therefore

$$\begin{aligned}ne_0(x) &= \sum_{i=0}^{n-1} x^i, \\ ne_1(x) &= 2m_1m_2 + \frac{n}{2(\varepsilon_1-\varepsilon_2)}(\varepsilon_1(x) - \varepsilon_2(x)) + \frac{1}{2}(\varepsilon_1(x) + \varepsilon_2(x)) - m_1\varepsilon_3(x) - m_2\varepsilon_4(x), \\ ne_2(x) &= 2m_1m_2 - \frac{n}{2(\varepsilon_1-\varepsilon_2)}(\varepsilon_1(x) - \varepsilon_2(x)) + \frac{1}{2}(\varepsilon_1(x) + \varepsilon_2(x)) - m_1\varepsilon_3(x) - m_2\varepsilon_4(x), \\ ne_3(x) &= -\sum_{i=0}^{n-1} x^i + p_2(1 + \varepsilon_4(x)), \\ ne_4(x) &= -\sum_{i=0}^{n-1} x^i + p_1(1 + \varepsilon_3(x)).\end{aligned}$$

For  $\alpha \in \mathbb{F}_{q^n}$  and  $m|n$ , let  $\text{Tr}_m^n(\alpha)$  be the trace of  $\alpha$  for extension  $\mathbb{F}_{q^n}/\mathbb{F}_{q^m}$ . We have, for  $E_i(x) = \phi(e_i(x))$ ,

$$\begin{aligned}
nE_0(\alpha) &= \text{Tr}_1^n(\alpha), \\
nE_1(\alpha) &= 2m_1m_2\alpha + \frac{1}{2} \sum_{\substack{r=1 \\ (r,n)=1}}^{n-1} \alpha^{q^r} - m_1(\text{Tr}_{p_1}^n(\alpha) - \alpha) - m_2(\text{Tr}_{p_2}^n(\alpha) - \alpha) \\
&\quad + \frac{n}{2(\varepsilon_1 - \varepsilon_2)} \left( \sum_{r=0}^{f-1} \alpha^{q^{q^r}} - \sum_{r=0}^{f-1} \alpha^{q^{sq^r}} \right), \\
nE_2(\alpha) &= 2m_1m_2\alpha + \frac{1}{2} \sum_{\substack{r=1 \\ (r,n)=1}}^{n-1} \alpha^{q^r} - m_1(\text{Tr}_{p_1}^n(\alpha) - \alpha) - m_2(\text{Tr}_{p_2}^n(\alpha) - \alpha) \\
&\quad - \frac{n}{2(\varepsilon_1 - \varepsilon_2)} \left( \sum_{r=0}^{f-1} \alpha^{q^{q^r}} - \sum_{r=0}^{f-1} \alpha^{q^{sq^r}} \right), \\
nE_3(\alpha) &= -\text{Tr}_1^n(\alpha) + p_2\text{Tr}_{p_1}^n(\alpha), \\
nE_4(\alpha) &= -\text{Tr}_1^n(\alpha) + p_1\text{Tr}_{p_2}^n(\alpha).
\end{aligned}$$

If  $2 \mid q$ , then

$$\mathcal{M}^{-1} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & \frac{n+1}{2} + \varepsilon_2 & \frac{n+1}{2} + \varepsilon_1 & m_1 & m_2 \\ 0 & \frac{n+1}{2} + \varepsilon_1 & \frac{n+1}{2} + \varepsilon_2 & m_1 & m_2 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

and

$$\begin{aligned}
E_0(\alpha) &= \text{Tr}_1^n(\alpha) \\
E_1(\alpha) &= m_1(\text{Tr}_{p_1}^n(\alpha) + \alpha) + m_2(\text{Tr}_{p_2}^n(\alpha) + \alpha) + \sum_{r=0}^{f-1} \alpha^{q^{q^r}} \\
E_2(\alpha) &= m_1(\text{Tr}_{p_1}^n(\alpha) + \alpha) + m_2(\text{Tr}_{p_2}^n(\alpha) + \alpha) + \sum_{r=0}^{f-1} \alpha^{q^{q^r}g} \\
E_3(\alpha) &= \text{Tr}_{p_1}^n(\alpha), \quad E_4(\alpha) = \text{Tr}_{p_2}^n(\alpha).
\end{aligned}$$

Then Theorem 2.2 implies the following result.

**Theorem 3.9.** Let  $p_1, p_2, p$  be distinct prime numbers,  $p_1 \geq 3, p_2 \geq 3, n = p_1p_2, q = p^m, f = \frac{(p_1-1)(p_2-1)}{2}, m_1 = \frac{p_1-1}{2}, m_2 = \frac{p_2-1}{2}$ . Suppose that  $(\mathbb{Z}/p_i\mathbb{Z})^* = \langle q \rangle$  ( $i = 1, 2$ ) and  $(p_1 - 1, p_2 - 1) = 2$ . We choose  $g \in \mathbb{Z}$  such that  $g \notin \langle q \rangle \subseteq (\mathbb{Z}/n\mathbb{Z})^*$ . Let  $\zeta$  be an  $n$ -th root of 1 in the algebraic closure of  $\mathbb{F}_q, \varepsilon_1 = \sum_{r=0}^{f-1} \zeta^{q^r}, \varepsilon_2 = \sum_{r=0}^{f-1} \zeta^{gq^r} = 1 - \varepsilon_1$ . For  $\alpha \in \mathbb{F}_{q^n}$  and  $m \mid n$ , let  $\text{Tr}_m^n(\alpha)$  be the trace mapping of  $\alpha$  for  $\mathbb{F}_{q^n}/\mathbb{F}_{q^m}$ .

(1) If  $2 \nmid q$ , then  $\alpha \in \mathbb{F}_{q^n}$  is a NBG for  $\mathbb{F}_{q^n}/\mathbb{F}_q$  if and only if

$$\text{Tr}_1^n(\alpha) \neq 0, \quad p_1\text{Tr}_{p_2}^n(\alpha), \quad p_2\text{Tr}_{p_1}^n(\alpha)$$

and

$$2m_1m_2\alpha + \frac{1}{2} \sum_{\substack{r=1 \\ (r,n)=1}}^{n-1} \alpha^{q^r} - m_1(\text{Tr}_{p_1}^n(\alpha) - \alpha) - m_2(\text{Tr}_{p_2}^n(\alpha) - \alpha) \\ \neq \pm \frac{n}{2(\varepsilon_1 - \varepsilon_2)} \left( \sum_{r=0}^{f-1} \alpha^{q^r} - \sum_{r=0}^{f-1} \alpha^{gq^r} \right).$$

(2) If  $2 \mid q$ , then  $\alpha \in \mathbb{F}_{q^n}$  is a NBG for  $\mathbb{F}_{q^n}/\mathbb{F}_q$  if and only if

$$\text{Tr}_1^n(\alpha) \neq 0, \quad \alpha \notin \mathbb{F}_{q^{p_i}} \quad (i = 1, 2)$$

and

$$m_1(\text{Tr}_{p_1}^n(\alpha) + \alpha) + m_2(\text{Tr}_{p_2}^n(\alpha) + \alpha) \neq \sum_{r=0}^{f-1} \alpha^{q^{r^c}} \quad (c = 1, g).$$

At the end of this section we show that the case  $p \mid n$  can be reduced into the case  $p \nmid n$ .

**Theorem 3.10.** Let  $n = p^l l$ ,  $(l, p) = 1$ ,  $t \geq 1$ ,  $q = p^m$  and  $\text{Tr}_l^n$  be the trace mapping for  $\mathbb{F}_{q^n}/\mathbb{F}_{q^l}$ . Then for  $\alpha \in \mathbb{F}_{q^n}$ ,  $\alpha$  is a NBG for  $\mathbb{F}_{q^n}/\mathbb{F}_q$  if and only if  $\text{Tr}_l^n(\alpha)$  is a NBG for  $\mathbb{F}_{q^l}/\mathbb{F}_q$ .

*Proof.* Let

$$x^l - 1 = f_1(x)f_2(x) \cdots f_r(x),$$

where  $f_i(x)$  ( $1 \leq i \leq r$ ) are distinct monic irreducible polynomials in  $\mathbb{F}_q[x]$ . Then  $x^n - 1 = (f_1(x)f_2(x) \cdots f_r(x))^{p^l}$  and Theorem 2.1 implies that

$$\begin{aligned} \alpha \text{ is a NBG for } \mathbb{F}_{q^n}/\mathbb{F}_q &\Leftrightarrow \alpha \text{ is not a root of } \varphi\left(\frac{x^n - 1}{f_i(x)}\right) \quad (1 \leq i \leq r) \\ &\Leftrightarrow \alpha \text{ is not a root of } \varphi(l_i(x)(1 + x^l + x^{2l} + \cdots + x^{(p^l-1)l})) \\ &\quad \text{where } l_i(x) = (x^l - 1)/f_i(x) \quad (1 \leq i \leq r) \\ &\Leftrightarrow \alpha \text{ is not a root of } L_i(x) \otimes (x + x^{q^l} + x^{q^{2l}} + \cdots + x^{q^{(p^l-1)l}}) \\ &\Leftrightarrow L_i(\text{Tr}_l^n(\alpha)) \neq 0 \quad (1 \leq i \leq r) \\ &\Leftrightarrow \text{Tr}_l^n(\alpha) \text{ is a NBG for } \mathbb{F}_{q^l}/\mathbb{F}_q. \end{aligned}$$

□

**Remark 3.11.** By combination of Theorem 3.10 and Theorem 3.2, we get the following result given by Peris [14].

**Corollary 3.12.** ([14]) Let  $q = p^l$  and  $n = p^s$  be powers of prime number  $p$  and  $l, s \geq 1$ . Then  $\alpha \in \mathbb{F}_{q^n}$  is a NBG for  $\mathbb{F}_{q^n}/\mathbb{F}_q$  if and only if  $\text{Tr}(\alpha) \neq 0$ , where  $\text{Tr}$  is the trace mapping for  $\mathbb{F}_{q^n}/\mathbb{F}_q$ .

### Acknowledgements

K.Feng's research was supported by the Tsinghua National Lab. for Information Science and Technology, and by the Science and Technology on Information Assurance Laboratory (No.KJ-12-01).

## References

- [1] D.W.Ash, I.F.Blake and S.A.Vanstone, Low complexity normal bases, *Discrete Appl.Math.*, 25 (1989), 191-210.
- [2] I.F.Blake, S.Gao and R.C.Mullin, Specific irreducible polynomial with linearly independent roots over finite fields, *Linear Algebra and Its Applications*, 253 (1997), 227-249.
- [3] M.Christopoulou, T.Garefalakis, D.Panario and D.Thomson, Gauss periods as constructions of low complexity normal bases, *Designs, Codes and Cryptograph*, 62 (2012), 43-62.
- [4] J.V Gathen and M.Giesbrecht, Constructing normal bases in finite fields, *J.Symbolic Computation*, 10 (1990), 547-570.
- [5] S.Gao, Abelian groups, Gauss periods and normal bases, *Finite fields and their applications*, 7 (2001), 149-164.
- [6] S.Gao and H.W.Lenstra, Optimal normal bases, *Designs, Codes and Cryptography*, 2 (1992), 315-323.
- [7] D.Jungnickel, T.Beth and W.Geiselman, A note of orthogonal circulant matrices over finite fields, *Arch.Math.*, 62 (1994), 126-133.
- [8] M.K.Kyuregyan, Iterated constructions of irreducible polynomials over finite fields with linearly independent roots, *Finite fields and their applications*, 10 (2004), 323-341.
- [9] Q.Liao, The Gaussian normal basis and its trace basis over finite fields, *Jour. of Number Theory*, 132 (2012), 1507-1518.
- [10] Q.Liao and K.Feng, On the complexity of the normal bases via prime Gauss period over finite fields, *Jour.Syst.Sci. and Complexity*, 22 (2009), 395-406.
- [11] P.Lidl and H.Niederreiter, *Finite fields*, Addison-Wesley, London, 1983.
- [12] Q.Liao and L.You, Low complexity of a class of normal bases over finite fields, *Finite fields and their applications*, 17 (2011), 1-14.
- [13] D.J.MacWilliams, Orthogonal circulant matrices over finite fields, and how to find them, *Jour.Combin. Theory (A)*, 10 (1971), 1-17.
- [14] S.Peris, Normal bases of cyclic fields of prime-power degree, *Duke Math.J.* 9(1942), 507-517.
- [15] D.Pei, C.C.Wang and J.K.Omura, Normal bases of finite field  $GF(2^m)^n$ , *IEEE Trans. Inform Theory*, 32 (1986), 285-287.
- [16] I.A.Samaev, Construction of polynomials irreducible over finite field with linearly independent roots, *Math. USSR sbornik*, 63 (1989), 507-519.
- [17] G.E.Séguin, Low complexity normal bases for  $\mathbb{F}_{2^{mn}}$ , *Discrete Appl.Math.*, 28 (1990), 309-312.
- [18] Z.X.Wan, *Lecture Notes on Finite Fields and Galois Rings*, World Scientific, Singapore, 2003.
- [19] M.Wang and I.F.Blake, Normal bases of finite fields  $GF(2^m)$  over  $GF(2)$ , *IEEE Trans. Inform Theory*, 43 (1997), 737-739.
- [20] B.Young and D.Panario, Low complexity normal bases in  $\mathbb{F}_{2^n}$ , *Finite fields and their applications*, 10 (2004), 53-64.